Learning Objectives
CS3600

Section 1 (Introduction)

1. The three aspects of data protection.
    a. How are secrecy and integrity the same?
    b. How is secrecy different from integrity?
    c. How is secrecy and integrity different from availability?
2. Access Control Policies
    a. What is an access control policy?
    b. Why should we be concerned that computers are enforcing them?
3. Assurance
    a. What is the difference between assurance and security features?
    b. How are policy and assurance related?
    c. How can assurance be increased?
    d. When is high assurance necessary?
    e. When is low assurance adequate?
4. Legal
    a. Why is the legal system having difficulty successfully prosecuting some kinds of computer crime?
    b. Why are some unethical acts not considered illegal?
5. Threats
    a. What is the relationship between threats and vulnerabilities?
    b. What is the relationship between threats and assurance?
    c. What is the biggest security problem?
6. Computer Security History
    a. Why was computer security so much better in the 1950's?
    b. What was the purpose of DoD Tiger Teams?
    c. What lesson(s) were learned by the efforts of the tiger teams?
    d. Why is "penetrate and patch" a flawed security methodology?
    e. What is the basis of the reference monitor concept?
    f. Why is it beneficial to group attacks into the different categories listed in the notes?
7. Vocabulary

Secrecy	Access Control Policy
Integrity	Security Function/Feature
Availability	Penetrate and Patch
Threat	Reference monitor
Vulnerability	Assurance
Tiger team	

Section 2 (Access Control I)

1. Insider / Outsider Threats
    a. What is the difference between trusted and trustworthy?
    b. What techniques are used to protect against malicious insiders?
    c. When does it make sense to do background checks on employees?
2. Identification & Authentication (I&A)
    a. What is the difference between Identification and Authentication?
    b. Why is I&A so important for the correct enforcement of access control policies?
    c. What are the three ways that users can be authenticated?
    d. In what environments should one consider using more than one way?
    e. Why isn't encryption enough to protect authentication data while traversing a network?
    f. What are Challenge and Response protocols trying to defend against?
    g. What is a Trusted Path, and what does it defend against?
3. Something You Know
    a. What are the advantages and disadvantages of passwords?
    b. What are the steps a system takes to verify a password?
    c. How is the password space calculated?
    d. How does a dictionary attack work? How can it be defeated?
    e. How does a brute force attack work? How can it be defended against?
    f. What are some system configuration items that help defend against password-based attacks (assuming they are available)?
    g. What is the difference between Proactive and Reactive enforcement?
4. Something You Have
    a. What are the advantages and disadvantages of tokens?
5. Something You Are
    a. What are the advantages and disadvantages of biometrics?
    b. Why is it possible for a biometric system to make the wrong decision when authenticating a user?
    c. Why is a false positive bad?
    d. Why is a false negative bad?
6. Discretionary Access Control (DAC)
    a. What are the defining characteristic(s) of a DAC policy?
    b. What are the advantages and disadvantages of ACLs?
    c. What are the advantages and disadvantages of Capability Lists?
    d. Why are DAC policies susceptible to Trojan horse attacks?

7. Vocabulary

Separation of Duties	Dictionary attack
Identification	Brute Force attack
Authentication	Password Space
I&A	Proactive
Token	Reactive
Biometrics	False Positive / Negative
Challenge/Response	Replay Attack
Call-back modems	Login Spoofing
DAC	Trusted Path
Trojan Horse	ACL

Section 3 (Access Control II)

1. Introductory material
    a. How is a MAC policy different from a DAC policy?
    b. What are two motivations for using a system that controls access to labeled data?
    c. Why is high assurance a good requirement for label-based systems storing multiple classifications of data, and supporting users with multiple clearances?
2. Bell and LaPadula secrecy model.
    a. How does the Confinement Property prevent unauthorized reading of data, if it is a rule which controls the writing of data?
    b. Given files and users with secrecy attributes (level and compartments), be able to determine which files the users can read and write.
3. Biba integrity model.
    a. If Biba is an integrity model, why does it have a rule for preventing high integrity users from reading low integrity data?
    b. Given files and users with integrity levels, be able to determine which files the users can read and write.
    c. Given files and users with both secrecy and integrity attributes, be able to determine which files the users can read and write.
4. Concluding MAC material
    a. How does the Bell and LaPadula model provide some defense against a Trojan horse?
    b. What benefit does a DAC policy provide on a system that also supports a MAC policy?
5. Covert Channels
    a. Why are covert channels a concern?
    b. What is the general approach behind the various exhaustion channels?
6. Multilevel Subjects
    a. Why are multilevel subjects necessary on a MAC-based system?
7. Supporting Policies
    a. What does Object Reuse defend against?
    b. Why is access control dependent upon I&A?
    c. Why is the following an odd combination for a system: a MAC secrecy policy and "weak" I&A?
8. Vocabulary

Mandatory Access Control (MAC)	Level
Label-based system	Compartment
Bell and LaPadula model	Integrity
Biba model	Multilevel subject
Confinement property (*-property)	Supporting policy
Covert Channel	Object Reuse
Session Level	

Section 4 (Building Secure Systems)

1. Reference Monitor
    a. What is the difference between “Security Functionality” and “Assurance”?
    b. What are the three requirements of a reference monitor?
    c. Explain why the removal of any one of the three requirements nullifies the reference monitor.
2. Protection of Memory
    a. What kind of memory protection does segmentation provide?
    b. What kind of memory protection does protection domains provide?
    c. What protection does a call gate provide?
    d. What is the minimum number of protection domains required for a high assurance system?
3. Principle of Least Privilege
    a. How does this principle apply to system design?
    b. How does modularity contribute to a better design?
    c. How does layering contribute to a better design?
4. Formal Methods Analysis
    a. How does formal methods analysis relate to assurance and policy?
    b. Why isn’t formal methods analysis performed more often on large software projects, such as operating systems?
    c. What are the four things that can contribute to the insecurity of a product?
    d. Which of the above four items can be mitigated using formal methods analysis?
5. Vocabulary

Trusted Computing Base (TCB)	Rings
Security Perimeter	Privilege Levels
Reference Monitor	Least Privilege
Segmentation	Security Model
Protection Domains	Formal Methods
	Call Gate

Section 5 (Malicious Software and Attacks)

1. Viruses
    a. How do program viruses spread?
    b. How do Word macro viruses spread?
    c. What is currently the most effective approach for detecting viruses?
    d. What are the advantages and disadvantages of detecting viruses using signatures?
    e. What are the advantages and disadvantages of detecting viruses with checksums or hashes?
    f. Why are heuristic approaches not a widely accepted approach for detecting viruses?
2. Worms
    a. What are the basic differences between a virus and a worm?
    b. Why are they potentially more dangerous than a virus?
    c. How do you defend against worms?
3. Packet Sniffing
    a. What are two ways to protect against packet sniffing?
4. Smurf Attack
    a. What is the result of a Smurf attack on the affected systems?
    b. How does the smurf attack work?
    c. How can it be defeated?
5. Social Engineering
    a. What techniques are used to prevent social engineering attacks from succeeding?
6. Vocabulary

Virus	Buffer Overflow
Worm	Smurf Attack
Backdoor	Social Engineering
Trapdoor	Denial of Service (DoS)
Packet Sniffing	Promiscuous mode

Section 6 (Evaluation, Certification & Accreditation)

1. Common Criteria
    a. What is the purpose of having system security evaluation standards?
    b. What are the two major categories of requirements provided by the Common Criteria?
    c. How is a PP intended to be used by customers?
    d. How is a PP intended to be used by a manufacturing community?
    e. How does a Security Target (ST) fit into the evaluation process?
    f. What is the assurance scale defined by the CC?
    g. Why do many consider the CC better than the Orange Book?
2. Certification and Accreditation (C&A)
    a. What is the difference between Evaluation and C&A?
    b. How is Certification different from Accreditation?
    c. What are the different operating modes, and how are they different?
    d. List four things that can cause a system to lose it's accreditation?
    e. What are the different types of risk analysis, and what are their advantages and disadvantages?
3. Vocabulary

Common Criteria (CC)	Designated Approving Authority (DAA)
Protection Profile (PP)	Operating Mode
Target of Evaluation (TOE)	Risk Analysis
Security Target (ST)	Annualized Loss Expectancy (ALE)
Evaluation Assurance Level (EAL)	Return on Investment (ROI)
Orange Book	

Section 7 (Basics of Cryptography)

1. Keys
    a. Given two choices: 1) keep the key secret; 2) keep the cipher secret. Which choice is better? Why?
    b. How is a brute force attack thwarted?
2. Substitution Ciphers
    a. What characteristic or property of the General Substitution Cipher allows it to be easily broken?
    b. Why are polyalphabetic ciphers significantly stronger than monoalphabetic ciphers?
    c. Why is the One-Time Pad immune to any kind of brute force attack?
    d. What are the three properties of a key for a true One-Time Pad?
    e. If the One-Time Pad offers "perfect" security, then why isn't it used widely?
3. Transposition Ciphers
    a. What is different about the frequency distribution produced by a transposition cipher when compared to a monoalphabetic substitution cipher?
4. Other Symmetric / Conventional Issues
    a. What are the basic "building blocks" of all modern symmetric ciphers?
    b. Why is the following sentence inaccurate: "The General Substitution Cipher is useless in today's modern world."
    c. Why is the distribution of symmetric keys challenging?
    d. Why is it wrong to say that a 128-bit key is twice as secure as a 64-bit key?
5. Data Encryption Standard (DES)
    a. How long is a DES key? How long is an AES key?
    b. Why do the DES S-boxes perform such a critical part in the security of DES?
    c. Why is CBC mode generally more secure than ECB mode?
    d. How does DES demonstrate good diffusion when operated in CBC mode?
    e. What is the expected use of the CFB and OFB modes?
6. Public Key (Asymmetric) Cryptography
    a. How is public key cryptography fundamentally different from private key (conventional / symmetric) cryptography?
    b. How does public key technology seem to solve key distribution problems?
    c. What are the steps for Alice to send a message to Bob if she only wants Bob to be able to read it?
    d. What are the steps for Alice to send a message to Bob if she wants him to be able to verify it came from her?
    e. RSA keys are so large they cannot be brute forced (in our lifetime). However, what is the potential weakness of the cipher?
    f. Asymmetric ciphers are based on difficult mathematical problems. Why is this a problem with their practical use?

7. Hashing
    a. Based solely on output size, a hashing function with a longer output is more secure than a shorter output. Why?
    b. What is the difference between a Hashing Function and a Message Authentication Code (MAC)?
    c. How can DES be used as a MAC?
8. Vocabulary

Conventional cryptography	DES (Data Encryption Standard)
Public key cryptography	IV (Initialization Vector)
Frequency distribution analysis	AES (Advanced Encryption Standard)
Digraph / Trigraph	Electronic Code Book mode
Monoalphabetic	Cipher Block Chaining mode
Polyalphabetic	Triple DES
One-Time Pad	RSA
Confusion	MD5
Diffusion	SHA

Section 8 (Cryptographic Protocols)

1. Protocols
    a. What are the three kinds of protocols?
    b. What are the advantages and disadvantages of each type?
2. Integrity Protocols
    a. When providing an integrity protocol, why is it necessary to encrypt either the message or the hash?
3. Services Using Conventional Cryptography
    a. List the steps for an integrity protocol using only conventional encryption.
    b. Why is the protocol for authenticity somewhat flawed?
4. Services Using Public Key Cryptography
    a. List the steps for providing secrecy.
    b. List the steps for providing integrity and authenticity.
    c. Why can't the recipient's public key be used to encrypt the hash?
    d. List the steps for providing a digital signature.
5. Key Distribution
    a. When distributing conventional keys, what are the three big problems?
    b. How do you determine the number of conventional keys you need if you need to communicate secretly (and separately) with N number of people?
    c. If the above situation was changed to require only public key encryption, how many keys will be generated in order to support secret communication between any two users?
    d. Conventional keys must be distributed secretly. What requirement do we place on the distribution of public keys?
    e. What problems arise with the use of a single KDC to distribute conventional keys?
    f. A hierarchy of KDCs solves the above problems, but introduces another concern. What is it?
    g. Using a hybrid approach, list the steps for Alice to communicate with Bob so that there is secrecy, integrity, authenticity, and efficiency.
    h. What problem do timestamps and nonces try to solve?
6. Vocabulary

Arbitrated	Digital Signature Standard (DSS)
Adjudicated	Non-Repudiation
Self-Enforcing	Key Distribution Center (KDC)
Digital Signature	Nonce

Section 9 (Network Security I)

1. Traffic Flow Analysis
    a. How can traffic flow analysis provide information when the actual messages cannot be read?
    b. What are two common approaches that are used to reduce the information obtained through traffic flow analysis?
2. Be able to answer the questions listed below for End-to-End Encryption, Link Encryption, and Virtual Private Networks.
    a. Are messages readable in the public network?
    b. Are messages readable in the private network?
    c. Are messages subject to traffic-flow analysis? How?
    d. Who is responsible for managing the encryption keys?
    e. Who decides when a message will be encrypted?
3. End-to-End Encryption
    a. What are the defining characteristics of end-to-end encryption?
    b. What are the advantages and disadvantages of using end-to-end encryption?
4. Link Encryption
    a. What are the defining characteristics of link encryption?
    b. Why does link encryption provide more protection from traffic flow analysis than end-to-end encryption?
    c. What kind of information is still available to traffic flow analysis when link encryption is used?
    d. What are the disadvantages of using link encryption?
5. Virtual Private Network (VPN)
    a. What two costs drove the development of VPN technology?
    b. If the IP header is still visible in the Internet, why does a VPN offer more protection from traffic flow analysis than end-to-end encryption?
6. Vocabulary

Circuit Switched Network	Traffic Flow Analysis
Packet Switched Network	End-to-End Encryption
Packet	Link Encryption
Packet Header	Virtual Private Network

Section 10
(Network Security II – TCP/IP, Firewalls and IDSs)

1. TCP/UDP port numbers
    a. When a client requests something from a server, what does the destination port number in the resulting packet correspond to?
    b. What does the source port (in the above question) correspond to?
    c. What significance is usually placed on port numbers less than 1024?
2. TCP and UDP
    a. What does it mean to say that TCP is a connection oriented protocol?
    b. What does it mean to say that UDP is a connectionless protocol?
    c. Under what circumstances would UDP be a better choice than TCP?
    d. How does the TCP handshake provide security as a side-effect?
    e. At what point in the handshake would you see a packet with the SYN flag set and the ACK bit not set?
3. Firewalls
    a. How does a firewall enforce the principle of least privilege?
    b. Why is a firewall considered an access control device?
    c. What are the disadvantages (if any) of using a firewall?
    d. What are the two philosophies that a firewall can have with respect to access control, and which one is more secure?
    e. Why is a dynamic packet filter considered better than a static packet filter?
    f. What benefit do application gateways provide?
4. Intrusion Detection System (IDS)
    a. How is an IDS similar to a virus scanner?
    b. What conclusions can be drawn about any technology that uses signatures?
    c. What are the advantages and disadvantages of host-based IDSs?
    d. What are the advantages and disadvantages of network-based IDSs?
    e. What are the advantages and disadvantages of distributed sensor IDSs?
5. Vocabulary

Transmission Control Protocol (TCP)	Demilitarized Zone (DMZ)
Internet Protocol (IP)	Intrusion Detection System (IDS)
User Datagram Protocol (UDP)	Host-Based IDS
TCP/UDP ports	Network-Based IDS
TCP Three-Way Handshake	Distributed Sensor IDS
Firewall	Honey Pot
Static Packet Filter	
Dynamic Packet Filter	
Application Gateway	

Section 11
(Network Security III – Public Key Infrastructure)

1. Public Key Distribution
    a. What problem(s) are we trying to solve with any kind of public key distribution scheme?
    b. Under what circumstances is a decentralized approach to public key distribution acceptable? Unacceptable?
    c. What role does a Certificate Authority play in a Public Key Infrastructure (PKI)?
    d. What key is used to verify that a public key certificate is valid?
    e. How is the above key obtained?
2. Certificate usage
    a. List the steps taken by Alice and Bob, if Alice wants to send a message to Bob secretly, assuming Alice just downloaded Bob's certificate from a web site. Assume the need to use conventional encryption to encrypt the message.
    b. List the steps Bob should take after he receives a signed message from Alice, assuming Bob just downloaded Alice's certificate from a web site.
    c. What are the advantages and disadvantages to the different approaches to saving private keys?
3. PKI Issues / Details
    a. Of all the keys managed by individuals and authorities in a PKI, which one individual key needs to be protected more than any other key?
    b. Why are Local Registration Authorities necessary?
    c. What role does the X.509 standard play in a PKI?
    d. Why is a mechanism like a Certification Revocation List (CRL) necessary?
    e. Why can it be necessary to issue every user two pairs of public/private keys?
4. Vocabulary

Certificate Authority	Certificate Revocation List (CRL)
Public Key Certificates	Key Escrow
Registration Authorities	Certificate Chains
X.509	Cookies